

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-V-

JOSHUA ADAM SCHULTE,

Defendant.

17-CR-548 (JMF)

ORDER


JESSE M. FURMAN, United States District Judge:

On November 12, 2021, the Court invited the parties to submit proposed modifications to the Protective Orders Pertaining to Classified Information previously entered in this case, ECF Nos. 61, 75. *See* ECF No. 585. After reviewing the Government’s and standby counsel’s most recent submissions, *see* ECF Nos. 670 and 689, and considering the objections made by Defendant on the record at the February 14, 2022 conference, the Court proposes entering a modified Protective Order to replace both previous orders.

Attached at **Exhibit A** is a clean copy of the Court’s DRAFT Amended Protective Order. Attached at **Exhibit B** is a redline showing the differences between the DRAFT Amended Protective Order and the version proposed by the Government on January 7, 2022, *see* ECF No. 670-2. The parties may file any further objections or suggestions by **March 4, 2022**. After that date, the Court may enter the Order without further notice.

SO ORDERED.

Dated: February 18, 2022
New York, New York



 JESSE M. FURMAN
 United States District Judge

Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (JMF)

**AMENDED PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION**

WHEREAS on August 16, 2018, the Court entered a Protective Order Pertaining to Classified Information (Dkt. Entry No. 61);

WHEREAS on December 12, 2018, the Court entered a Supplemental Protective Order Pertaining to Classified Information (Dkt Entry No. 75);

WHEREAS on July 26, 2021, the Court entered an Opinion and Order granting the Defendant's motion to waive his Sixth Amendment right to counsel and to proceed *pro se*, and further appointing the Defendant's former counsel as standby counsel in this matter;

NOW THEREFORE IT IS HEREBY ORDERED that this Protective Order Pertaining to Classified Information supersedes the August 16 and December 12, 2018 orders. The Court finds that the terms of this Order are authorized by Section 3 of the Classified Information Procedures Act ("CIPA"), the "Revised Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information" (hereinafter "Security Procedures," which are reprinted after CIPA § 9), Rules 16 and 57 of the Federal Rules of Criminal Procedure, and the general supervisory powers of the Court, and are necessary to protect the national security and to conform the procedures governing the storage,

handling, and control of classified information in this matter to the Defendant's *pro se* status and the appointment of standby counsel.¹

1. The Court finds that this case will involve information that has been classified in the interest of national security. The storage, handling, and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to this information requires appropriate security clearances and need-to-know, as set forth in Executive Order 13256 (or successor order), that has been validated by the government.² The purpose of this Order is to establish procedures that counsel and the parties must follow in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information and may be modified from time to time by further Order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

2. Definitions. The following definitions shall apply to this Order:

a. "Defense" or "defense team" refers collectively to the Defendant's standby counsel and any support staff, investigators, or experts assisting the Defendant or the Defendant's standby counsel authorized to receive classified information pursuant to this Order.

b. "Classified information" shall include:

i. Any document, recording, or information, regardless of its origin and including information acquired or conveyed orally, that has been classified by any Executive

¹ The Court understands that the Government may move for a supplemental protective order depending on the nature of additional information that is determined to be discoverable.

² Any individual to whom classified information is disclosed pursuant to this Order shall not disclose such information to another individual unless the U.S. agency that originated that information has validated that the proposed recipient possesses an appropriate security clearance and need to know.

Branch agency in the interests of national security pursuant to Executive Order 13526, as amended, or its predecessor or successor orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION” (“SCI”); and

ii. Any document, recording, or information now or formerly in the possession of a private party, regardless of its origin and including information acquired or conveyed orally, that (A) has been derived from information that was classified by the United States Government, and/or (B) has been classified by the United States Government as set forth above.

c. “Document,” “materials,” and “information” shall include, but are not limited to:

i. all written, printed, visual, digital, electronic, or audible matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), as well as metadata;

ii. notes (handwritten, oral, or electronic); papers; letters; correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings, or other communications; bulletins; teletypes; telecopies; telegrams; telexes; transcripts; cables; facsimiles; invoices; worksheets and drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer

tapes, disks, or thumb drives and all manner of electronic data-processing storage; and alterations, modifications, changes, and amendments of any kind to the foregoing; and

iii. information acquired, conveyed, or obtained orally.

d. “Access to classified information” shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

e. “Secure Area” shall mean a sensitive compartmented information facility (“SCIF”) approved by a designated Classified Information Security Officer (“CISO”) for the storage, handling, and control of classified information.

Classified Information

3. All classified information that the Court or Government approves for limited authorized disclosure to the defense or the Defendant shall contain an appropriate classification marking and be marked “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (JMF).”

4. All classified documents, and classified information contained therein, shall remain classified unless the documents bear a clear indication that they are not classified or have been declassified by the agency or department that originated the document or information contained therein (“originating agency”).

5. All access to classified information shall conform to this Order and the Memorandum of Understanding described herein.

6. Any classified information provided to the defense or the Defendant by the government is to be used solely by the defense and the Defendant and solely for the purpose of preparing the defense. The defense and the Defendant may not disclose or cause to be disclosed in

connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

7. The defense may not disclose classified information to the Defendant unless that same information has been previously disclosed to the defense by the Defendant or unless the Government has approved its release to the Defendant and marked it “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (JMF).” The defense may not confirm or deny to the Defendant the assertions made by the Defendant based on knowledge the defense may have obtained from classified information, except where that classified information has been provided to the Defendant pursuant to this Order. Any classified information the defense discloses to or discusses with the Defendant in any way shall be handled in accordance with this Order and the attached Memorandum of Understanding, including such requirements as confining all discussions, documents, and materials to an accredited SCIF.

8. The defense and the Defendant shall not disclose classified information to any person, except to the Court, government personnel who hold appropriate security clearances and have been determined to have a need to know that information, and those specifically authorized to access that information pursuant to this Order.

9. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who, by virtue of this Order or any other court order, are granted access to classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the defense or the Defendant to have such information confirmed

or denied at trial or in any public proceeding in this case, the defense and the Defendant must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

10. In the event that classified information enters the public domain, the defense and the Defendant are precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that the defense or the Defendant had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. If there is any question as to whether information is classified, the defense and the Defendant must handle that information as though it is classified unless Government counsel or the CISO confirms that it is not classified.

Security Procedures

11. In accordance with the provisions of CIPA and the Security Procedures, the Court has designated Daniel Hartenstine as the CISO for this case for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified information that has been made available to the defense or the Defendant in connection with this case. The defense and the Defendant shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information. Daniella M. Medel, Matthew W. Mullery, Carli V. Rodriguez-Feo, Harry J. Rucker, and Winfield S. Slade have been designated as alternate CISOs in the event that Mr. Hartenstine is not available.

12. The Government has advised the Court that Assistant United States Attorneys David W. Denton, Jr. and Michael D. Lockard, as well as their supervisors (“Government

counsel”), have the security clearances allowing them to have access to classified information that Government counsel intend to use, review, or disclose in this case.

13. The Court has been advised, through the CISO, that the Defendant’s standby counsel, Sabrina Shroff and Deborah Colson, have been granted security clearances permitting them to have access to the classified information that Government counsel intend to use and disclose pursuant to this Order.

14. *Protection of Classified Information.* The Court finds that to protect the classified information involved in this case, to the extent that Ms. Shroff and Ms. Colson have the requisite security clearances and a “need to know” the classified information, they shall be given authorized access to classified national security documents and information as required by the Government’s discovery obligations and subject to the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding attached hereto, and any other Orders of this Court.

15. The Defendant has a continuing contractual obligation to the Government not to disclose to any unauthorized person classified information known to him or in his possession. The Government is entitled to enforce that agreement to maintain the confidentiality of classified information. Moreover, because the allegations in this case involve breaches of agreements the Defendant entered into regarding the handling of classified information, the Defendant must sign the Memorandum of Understanding. In addition, the Defendant is subject to this Court’s authority, contempt powers, and other authorities, and shall fully comply with the nondisclosure agreements he has signed, this Order, the Memorandum of Understanding, and applicable statutes.

16. The signed Memorandum of Understanding shall be filed with the Court, and executed copies of the Memorandum of Understanding shall be served upon the Government. The

substitution, departure, or removal for any reason from this case of standby counsel for the Defendant or any other member of the defense, shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

17. Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, no court personnel required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first have received the necessary security clearance as determined by the CISO.

18. Any additional persons whose assistance the defense or the Defendant reasonably requires may have access to classified information in this case only if they are granted an appropriate security clearance through the CISO, obtain approval from this Court with prior notice of the identity of the additional persons to the U.S. government agency that originated the information, and satisfy the other requirements described in this Order for access to classified information.

19. An individual with a security clearance and a need to know as determined by any government entity is not automatically authorized to disclose any classified information to any other individual, even if that other individual also has a security clearance. Rather, any individual who receives classified information may disclose that information only to an individual who has been determined by an appropriate government entity to have both the required security clearance and a need to know the information.

20. *Secure Areas for the Defense.* The Court is informed that the Federal Bureau of Investigation (“FBI”), U.S. Marshals Service (“USMS”), and CISO have arranged for approved Secure Areas for use by the defense and the Defendant. The CISO shall establish procedures to

assure the Secure Areas are accessible during business hours to the defense, and at other times upon reasonable request as approved by the CISO in consultation with the FBI and USMS. The Secure Areas contain a working area for the defense and the Defendant and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defense. The CISO, in consultation with standby counsel for the Defendant, USMS, and FBI, shall establish procedures to assure that the Secure Areas are maintained and operated in the most efficient manner consistent with the protection of classified information and in compliance with accreditation requirements. No classified documents, material, recordings, or other information may be removed from the Secure Areas unless so authorized by the CISO. The CISO shall not reveal to the Government the content of any conversations they may hear among the defense, nor reveal the nature of the documents being reviewed, or the work being generated. The presence of the CISO shall not operate to render inapplicable the attorney-client privilege.

21. *Review of Defense Filings.* The Defendant's *pro se* status does not affect or relieve in any way standby counsel's independent obligation to ensure that documents or pleadings containing classified information are filed in accordance with the provisions of this Order. In particular, standby counsel shall review all proposed filings of the Defendant for possible classified information before publicly filing any document. If standby counsel is unable reasonably to determine whether a filing contains or likely contains classified information, standby counsel shall contact the CISO and/or file the document as presumptively classified pending classification review pursuant to the provisions of this Order. Unless and until the CISO or the Government advise standby counsel that the document is unclassified, standby counsel shall treat the document as presumptively classified.

22. *Filing of Papers by the Defense.* Any pleading or other document filed by the defense or the Defendant that the Defendant or standby counsel for the Defendant knows or reasonably should know contains classified information as defined in paragraph 2(b), shall be filed as follows:

a. The document (along with a courtesy electronic copy on CD or DVD) shall be filed by standby counsel under seal with the CISO or an appropriately cleared designee identified by the CISO and shall be marked, “Filed in Camera and Under Seal with the Classified Information Security Officer.” The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 4:00 p.m. Within a reasonable time after making a submission to the CISO, the defense shall file on the public record in the CM/ECF system a “Notice of Filing” notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall consult with representatives of the agency or agencies having the relevant classification authority in order to determine whether the pleading or document contains classified information. If the agency or agencies with classification authority determine that the pleading or document contains classified information, the CISO shall ensure the document is marked with the appropriate classification marking and remains under seal. The CISO shall immediately deliver or, if required, arrange for delivery by an appropriately cleared designee under seal to the Court and Government counsel any pleading or document to be filed by the defense that contains classified information, unless the pleading or document is an *ex parte* filing.

23. *Filing of Papers by the Government.* Any pleading or other document filed by the Government that Government counsel knows or reasonably should know contains classified information as defined in paragraph 2(b), shall be filed as follows:

a. The document (along with a courtesy electronic copy on CD or DVD) shall be filed under seal with the CISO or an appropriately cleared designee and shall be marked, “Filed in Camera and Under Seal with the Classified Information Security Officer.” The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 4:00 p.m. Within a reasonable time after making a submission to the CISO, Government counsel shall file on the public record in the CM/ECF system a “Notice of Filing” notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall ensure the document is marked with the appropriate classification marking and remains under seal. The CISO shall immediately deliver under seal or, if required, arrange for delivery by an appropriately cleared designee to the Court and to the Secure Area used by the defense and the Defendant any pleading or document to be filed by the Government that contains classified information, unless the pleading or document is an *ex parte* filing.

24. *Record and Maintenance of Classified Filings.* The CISO shall maintain a separate sealed record for those materials that are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

25. *Classification Review.* With respect to classified filings described in paragraphs 22(b) and 23(b), except *ex parte* filings or filings under seal, and with respect to classified orders

of the Court, the agency having relevant classification authority shall conduct a classification review and prepare a redacted version of the filings and orders for public filing on the docket. Unless and until the Court orders otherwise, the classification review shall be completed (i) for filings and orders of 10 pages or fewer, within one week; (ii) for filings and orders of 25 pages or fewer, within two weeks; and (iii) for filings of greater than 25 pages, within three weeks. Attachments containing classified information will not be subject to classification review and will be filed under seal, unless otherwise ordered by the Court. Any attachments subject to classification review will be included in the page counts above, except documents that have previously undergone classification review. These time periods shall begin to run upon the agency receiving the document from the CISO or from Government counsel. The Government shall promptly notify the Court if a particular classification review cannot reasonably be completed within these time periods and may request additional time. The Court may shorten the timeframes set forth above as this case gets closer to trial.

26. *The Classified Information Procedures Act.* Procedures for public disclosure of classified information in this case shall be those established by CIPA. The defense and the Defendant shall comply with the requirements of CIPA Section 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the defense and the Defendant shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to Government counsel and until the Government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the Government to appeal any adverse determination under CIPA Section 7 has expired or any appeal under Section 7 by the Government

is decided. Pretrial conferences involving classified information shall be conducted *in camera* in the interest of the national security, be attended only by persons granted access to classified information and a need to know, and the transcripts of such proceedings shall be maintained under seal.

27. *Access to Classified Information.* In the interest of the national security, representatives of the defense granted access to classified information and the Defendant shall have access to classified information only as follows:

a. All classified information produced by the Government to counsel for the Defendant in discovery or otherwise, and all classified information possessed, created or maintained by the defense or the Defendant, including notes and any other work product, shall be stored, maintained and used only in the Secure Areas established by the FBI and CISO, unless otherwise authorized by the CISO.

b. *Special procedures for audio recordings.* Any classified audio recordings that the Government discloses to the defense or the Defendant shall be maintained by the FBI and CISO in the Secure Areas. Such recordings may be reviewed only on a stand-alone, non-networked computer or other device within the Secure Areas that does not have the capability to duplicate or transmit information. The defense or the Defendant must use headphones to review such recordings and the headphones must be wired and not have any wireless capability.

c. The defense shall have free access to the classified information made available to them, and the Defendant shall have free access to the classified information made available to him in accordance with the provision of this Order, in the Secure Areas established by

the FBI and CISO and shall be allowed to take notes and prepare documents with respect to those materials.

d. No representative of the defense (including but not limited to standby counsel, investigators, paralegals, translators, experts, and witnesses) or the Defendant shall copy or reproduce any classified information in any manner or form, except with the approval of the CISO and in accordance with the procedures established by the CISO for the operation of the Secure Area.

e. All documents prepared by the defense or the Defendant (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in the Secure Areas on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, thumb drives, discs, CDs, DVDs exhibits, and electronic or digital copies) that may contain classified information shall be maintained in the Secure Areas unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to Government counsel or any other party.

f. The defense and the Defendant shall discuss classified information only within the Secure Areas or in an area authorized by the CISO.

g. The defense and the Defendant shall not disclose, without prior approval of the Court, classified information to any person not named in this Order except to the Court, Court personnel, and government personnel identified by the CISO as having the appropriate clearances and the need to know. Government counsel shall be given an opportunity to be heard in response

to any defense or Defendant's request for disclosure to a person not identified in this Order. Any person approved by this Court for access to classified information under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to this Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, the Department of Justice shall promptly seek to obtain security clearances for them at the request of standby counsel or the Defendant. As set forth above, the defense and the Defendant shall not disclose classified information, even to an individual with the appropriate security clearance, without following the procedure referenced in paragraph 18.

h. The defense and the Defendant shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the Internet and email, or in the presence of any person who has not been granted access to classified information by the Court.

i. Any documents written by the defense or the Defendant that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

j. The defense shall not disclose classified information to the Defendant—other than materials marked “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (JMF)”—absent written permission from the Government.

28. *Contacting U.S. Intelligence Agency Employees.* The employment and/or affiliation of certain individuals with a U.S. Intelligence Agency and/or their responsibilities at the U.S. Intelligence Agency may constitute classified or highly sensitive facts. As a result, if the defense or the Defendant would like to contact individuals who may be employed by or affiliated with a U.S. Intelligence Agency (“Intelligence Agency Employees”), the following procedures apply:

a. The CISO is the point of contact for the purpose of facilitating contact between the defense or the Defendant and Intelligence Agency Employees. If the defense or the Defendant would like to contact Intelligence Agency Employees, the name of any such person must be provided to the CISO through properly secured channels.

b. The CISO will subsequently contact via a secure line a designated employee or employees (the “Designated Employee(s)”) at the U.S. Intelligence Agency who will be walled off from the prosecution team. The Designated Employee(s) will notify the Intelligence Agency Employee of the defense or the Defendant’s request to contact and/or interview him or her.

c. If an Intelligence Agency Employee agrees to be contacted and/or interviewed by the defense, the CISO will coordinate with the defense and with the Intelligence Agency Employee regarding logistics (e.g., timing and location) of the proposed interview(s). Classified information may be discussed with the Intelligence Agency Employees only in a SCIF or via secure telephonic or video communications.

29. Any unauthorized disclosure or mishandling of classified information may constitute violations of federal criminal law. In addition, any violation of the terms of this Order shall be brought immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may also result

in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention, or handling of classified documents or information could cause serious damage, and in some cases exceptionally grave damage to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. The purpose of this Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it.

30. All classified documents and information to which the defense or the Defendant have access in this case are now and will remain the property of the United States. Upon request by the CISO, all persons shall return to the CISO all classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information. The notes, summaries, and other documents prepared by the defense or the Defendant that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of the case. At the conclusion of this case, including any appeals or ancillary proceedings thereto, all such notes, summaries, and other documents are to be destroyed by the CISO in the presence of standby counsel for the Defendant if they choose to be present. Even upon the conclusion of this case, the parties, counsel, and any of their representatives or associates to whom classified documents or information was disclosed, remain obligated to protect against the unauthorized disclosure of any classified information learned during the course of the proceedings, as described herein.

Procedures Relating to the Defendant's Access to the Secure Areas

31. The schedule for the Defendant's visits to the Courthouse SCIF are to be coordinated among the USMS, the FBI, the U.S. Attorney's Office, and standby counsel, and the CISO and the Court are to be notified of the schedule. Standby counsel or a cleared paralegal under the direction and supervision of standby counsel shall be reasonably available to the Defendant when he is in the Secure Area in order to, among other things, facilitate his access to Classified Information in order to prepare his defense.

32. The Secure Area contains equipment (the "Computer Equipment") to allow the Defendant and cleared standby counsel to review the Classified Information produced by the Government. The Computer Equipment shall be used only for purposes of preparing the defense, and is enabled to log computer activity occurring on the equipment and is equipped with security measures. These logs may be reviewed by law enforcement agents or personnel who are not involved in the prosecution of the Defendant (the "Wall Team"). In the event the Wall Team determines the Computer Equipment has been used in an unauthorized manner, including by attempting to circumvent any security measures or logging features, the Wall Agent will report that information to the CISO, who will notify the Court for further action.

33. When the Defendant is present in the Secure Area, the Secure Area will be monitored for security purposes through closed circuit television ("CCTV") by the Marshals and an authorized FBI agent for all scheduled productions. The CCTV will allow only for visual monitoring of the Defendant and cleared defense counsel, and will not include audio. The CCTV will not be recorded. Should any Marshal or FBI agent hear any conversation between the Defendant and any of his counsel, those conversations will not be communicated to any member

of the government prosecution team, including, but not limited to attorneys, agents, and support staff.

34. Unless the Court orders otherwise, the Defendant will be subject to appropriate security measures to be determined by USMS during the time he is in the SCIF. The Defendant will be stripped searched after departing the SCIF at the conclusion of each session. The USMS may terminate any session if security issues arise during the session.

35. On September 23, 2021, the Court issued an Order (Dkt. Entry No. 518) directing, among other things, that the parties schedule and hold a telephone call twice a month to meet and confer about discovery and other issues, to take place at a mutually convenient time during the Defendant's regularly scheduled SCIF hours and with the participation of standby counsel at the discretion of the Defendant and standby counsel. These calls may be held using a teleconference facility and may be recorded by the Government. *See also* Dec. 20, 2021 Tr. at 38-40. The Defendant may not personally place or receive phone calls from the SCIF and shall only use the SCIF phone with the assistance of standby counsel or cleared staff working on this matter at the direction and under the supervision of standby counsel, who will place and receive calls for the Defendant. Standby counsel or cleared staff working on this matter at the direction and under the supervision of standby counsel shall assist the Defendant in joining teleconference calls directed by the September 23, 2021 Order and this Order. The Government will endeavor to identify the dates of these calls in advance upon receiving the Defendant's SCIF schedule from the USMS, and may schedule such a call by giving at least 24 hours' notice to standby counsel or by any other means that reasonably gives the Defendant notice. As directed above, the Defendant shall not

disclose classified information on telephone calls that are not cleared for classified communications.

Concluding Provisions

36. Nothing contained in this Order shall be construed as a waiver of any right of the Defendant. No admission made by the Defendant or his standby counsel during pretrial conferences may be used against the Defendant unless it is in writing and signed by the Defendant. *See* CIPA § 2.

37. A copy of this Order shall be issued forthwith to standby counsel for the Defendant who shall be responsible for advising the Defendant and representatives of the defense of the contents of this Order. Standby counsel for the Defendant, the Defendant, and any other representatives of the defense who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 15 of this Order, and the Defendant and standby counsel for the Defendant shall file executed originals of such documents with the Court and the CISO and serve an executed original upon the government. The execution and filing of the Memorandum of Understanding is a condition precedent for the Defendant, standby counsel for the Defendant, and any other representative of the defense to have access to classified information.

Dated: February 18, 2022
New York, New York

SO ORDERED:

THE HONORABLE JESSE M. FURMAN
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (JMF)

**MEMORANDUM OF UNDERSTANDING REGARDING RECEIPT OF
CLASSIFIED INFORMATION**

Having familiarized myself with the applicable statutes, regulations, and orders, including but not limited to, Title 18, United States Code, Sections 793, 794, 798, and 1924; the Intelligence Identities Protection Act, Title 50, United States Code, Section 3121 ; Title 18, United States Code, Section 641; Title 50, United States Code, Section 783; and Executive Order 13526, I understand that I may be the recipient of information and documents that concern the present and future security of the United States and which belong to the United States, and that such documents and information together with the methods and sources of collecting it are classified by the United States Government. In consideration for the disclosure of classified information and documents:

(1) I agree that I shall never divulge, publish, or reveal either by word, conduct or any other means, such classified documents and information unless specifically authorized in writing to do so by an authorized representative of the United States Government; or as expressly authorized by the Court pursuant to the Classified Information Procedures Act and any Protective Order entered in United States v. Joshua Adam Schulte, S3 17 Cr. 548 (JMF).

(2) I agree that this Memorandum will remain forever binding on me.

(3) I have received, read, and understand the Amended Protective Order Regarding Classified Information entered by the United States District Court for the Southern District of New York on _____, 2022, in United States v. Joshua Adam Schulte, S3 17 Cr. 548 (JMF), relating to classified information, and I agree to comply with the provisions thereof.

(4) I understand that any prior contractual obligations that may bind me to continue to protect classified information remain in full force and effect, and are not superseded by this Memorandum of Understanding. Additionally, I understand that this Memorandum of Understanding does not absolve me of any criminal or civil penalties that may otherwise be imposed upon me as a result of my unauthorized disclosure of classified information.

Sabrina Shroff, Esq.
Standby Counsel for the Defendant

Date

Deborah Colson, Esq.
Standby Counsel for the Defendant

Date

Joshua Adam Schulte
Defendant

Date

Exhibit B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (JMF)

AMENDED PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION

WHEREAS on August 16, 2018, the Court entered a Protective Order Pertaining to Classified Information (Dkt. Entry No. 61);

WHEREAS on December 12, 2018, the Court entered a Supplemental Protective Order Pertaining to Classified Information (Dkt Entry No. 75);

WHEREAS on July 26, 2021, the Court entered an Opinion and Order granting the ~~defendant's~~Defendant's motion to waive his Sixth Amendment right to counsel and to proceed *pro se*, and further appointing the ~~defendant's~~Defendant's former counsel as standby counsel in this matter;

NOW THEREFORE IT IS HEREBY ORDERED that this Protective Order Pertaining to Classified Information supersedes the ~~provisions of~~ August 16 and December 12, 2018 orders. The Court finds that the terms of this Order are authorized by Section 3 of the Classified Information Procedures Act ("CIPA"), the "Revised Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information" (hereinafter "Security Procedures," which are reprinted after CIPA § 9), Rules 16 and 57 of the Federal Rules of Criminal Procedure, and the general supervisory powers of the Court, and ~~is~~are necessary to protect the national security and to conform the procedures governing

the storage, handling, and control of classified information in this matter to the ~~defendant's~~Defendant's *pro se* status and the appointment of standby counsel.¹

1. The Court finds that this case will involve information that has been classified in the interest of national security. The storage, handling, and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to this information requires appropriate security clearances and need-to-know, as set forth in Executive Order 13256 (or successor order), that has been validated by the government.² The purpose of this Order is to establish procedures that counsel and the parties must follow in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information and may be modified from time to time by further Order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

2. Definitions. The following definitions shall apply to this Order:

a. “Defense” or “defense team” refers collectively to the Defendant’s standby counsel and any support staff, investigators, or experts assisting the Defendant or the Defendant’s standby counsel authorized to receive classified information pursuant to this Order.

b. “Classified information” shall include:

i. Any document, recording, or information, regardless of its origin and including information acquired or conveyed orally, that has been classified by any Executive

¹ The Court understands that the Government may move for a supplemental protective order depending on the nature of additional information that is determined to be discoverable.

² Any individual to whom classified information is disclosed pursuant to this Order shall not disclose such information to another individual unless the U.S. agency that originated that information has validated that the proposed recipient possesses an appropriate security clearance and need to know.

Branch agency in the interests of national security pursuant to Executive Order 13526, as amended, or its predecessor or successor orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION” (“SCI”); and

ii. Any document, recording, or information now or formerly in the possession of a private party, regardless of its origin and including information acquired or conveyed orally, that (A) has been derived from information that was classified by the United States Government, and/or (B) has been classified by the United States Government as set forth above;

~~iii. Verbal or other unwritten or unrecorded information known to the defendant or the defense team that has been classified by the United States Government as set forth above;~~

~~iv. Any information, regardless of its origin, that the defense knows contains classified information, including information acquired or conveyed orally;~~

~~v. Any document, recording, or information as to which the defense has been notified orally or in writing contains classified information; and~~

~~3.1. Any document, recording, or information that is classified, as set forth in subparagraph (i), above, and that the Court or Government has approved for limited authorized disclosure to the defendant pursuant to the restrictions set forth herein. All classified information that the Court or Government approves for limited authorized disclosure to the defendant will contain an appropriate classification marking and will be marked “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3-17-Cr-548 (JMF).”~~

c. “Document,” “materials,” and “information” shall include, but are not limited to:

i. all written, printed, visual, digital, electronic, or audible matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), as well as metadata;

ii. notes (handwritten, oral, or electronic); papers; letters; correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings, or other communications; bulletins; teletypes; telecopies; telegrams; telexes; transcripts; cables; facsimiles; invoices; worksheets and drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes, disks, or thumb drives and all manner of electronic data-processing storage; and alterations, modifications, changes, and amendments of any kind to the foregoing; and

iii. information acquired, conveyed, or obtained orally.

d. “Access to classified information” shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

e. “Secure Area” shall mean a sensitive compartmented information facility (“SCIF”) approved by a designated Classified Information Security Officer (“CISO”) for the storage, handling, and control of classified information.

Classified Information

3. All classified information that the Court or Government approves for limited authorized disclosure to the defense or the Defendant shall contain an appropriate classification marking and be marked “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (JMF).”

4. All classified documents, and classified information contained therein, shall remain classified unless the documents bear a clear indication that they are not classified or have been declassified by the agency or department that originated the document or information contained therein (“originating agency”).

5. All access to classified information shall conform to this Order and the Memorandum of Understanding described herein.

6. Any classified information provided to the defense or the Defendant by the government is to be used solely by the defense and the Defendant and solely for the purpose of preparing the defense. The defense and the Defendant may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

7. The defense may not disclose classified information to the Defendant unless that same information has been previously disclosed to the defense by the Defendant or unless the Government has approved its release to the Defendant and marked it “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (JMF).” The defense may not confirm or deny to the Defendant the assertions made by the ~~defendant~~Defendant based on knowledge the defense may have obtained from classified information, except where that classified information has been provided to the Defendant pursuant to this Order. Any classified

information the defense discloses to or discusses with the Defendant in any way shall be handled in accordance with this Order and the attached Memorandum of Understanding, including such requirements as confining all discussions, documents, and materials to an accredited SCIF.

8. The defense and the Defendant shall not disclose classified information to any person, except to the Court, government personnel who hold appropriate security clearances and have been determined to have a need to know that information, and those specifically authorized to access that information pursuant to this Order.

9. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who, by virtue of this Order or any other court order, are granted access to classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the defense or the Defendant to have such information confirmed or denied at trial or in any public proceeding in this case, the defense and the Defendant must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

10. In the event that classified information enters the public domain, the defense and the Defendant are precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that the defense or the Defendant had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. If there is any question as to whether information is classified, the defense and the

Defendant must handle that information as though it is classified unless Government counsel or the CISO confirms that it is not classified.

Security Procedures

11. In accordance with the provisions of CIPA and the Security Procedures, the Court has designated Daniel Hartenstine as the CISO for this case for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified information that has been made available to the defense or the Defendant in connection with this case. The defense and the Defendant shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information. Daniella M. Medel, Matthew W. Mullery, Carli V. Rodriguez-Feo, Harry J. Rucker, and Winfield S. Slade have been designated as alternate CISOs in the event that Mr. Hartenstine is not available.

12. The Government has advised the Court that Assistant United States Attorneys David W. Denton, Jr. and Michael D. Lockard, as well as their supervisors (“Government counsel”), have the security clearances allowing them to have access to classified information that Government counsel intend to use, review, or disclose in this case.

13. The Court has been advised, through the CISO, that the Defendant’s standby counsel, Sabrina Shroff and Deborah Colson, have been granted security clearances permitting them to have access to the classified information that Government counsel intend to use and disclose pursuant to this Order.

14. *Protection of Classified Information.* The Court finds that to protect the classified information involved in this case, to the extent that Ms. Shroff and Ms. Colson have the requisite security clearances and a “need to know” the classified information, they shall be given authorized

access to classified national security documents and information as required by the Government's discovery obligations and subject to the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding attached hereto, and any other Orders of this Court.

15. The Defendant has a continuing contractual obligation to the Government not to disclose to any unauthorized person classified information known to him or in his possession. The Government is entitled to enforce that agreement to maintain the confidentiality of classified information. Moreover, because the allegations in this case involve breaches of agreements the Defendant entered into regarding the handling of classified information, the Defendant must sign the Memorandum of Understanding. In addition, the Defendant is subject to this Court's authority, contempt powers, and other authorities, and shall fully comply with the nondisclosure agreements he has signed, this Order, the Memorandum of Understanding, and applicable statutes.

16. The signed Memorandum of Understanding shall be filed with the Court, and executed copies of the Memorandum of Understanding shall be served upon the Government. The substitution, departure, or removal for any reason from this case of standby counsel for the Defendant or any other member of the defense, shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

17. Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, no court personnel required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first have received the necessary security clearance as determined by the CISO.

18. Any additional persons whose assistance the defense or the Defendant reasonably requires may have access to classified information in this case only if they are granted an

appropriate security clearance through the CISO, obtain approval from this Court with prior notice of the identity of the additional persons to the U.S. government agency that originated the information, and satisfy the other requirements described in this Order for access to classified information.

19. An individual with a security clearance and a need to know as determined by any government entity is not automatically authorized to disclose any classified information to any other individual, even if that other individual also has a security clearance. Rather, any individual who receives classified information may disclose that information only to an individual who has been determined by an appropriate government entity to have both the required security clearance and a need to know the information.

20. *Secure Areas for the Defense.* The Court is informed that the Federal Bureau of Investigation (“FBI”), U.S. Marshals Service (“USMS”), and CISO have arranged for approved Secure Areas for use by the defense and the Defendant. The CISO shall establish procedures to assure the Secure Areas are accessible during business hours to the defense, and at other times upon reasonable request as approved by the ~~FBI and~~ CISO in consultation with the ~~FBI and~~ USMS. The Secure Areas contain a working area for the defense and the Defendant and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defense. The CISO, in consultation with standby counsel for the Defendant, USMS, and FBI, shall establish procedures to assure that the Secure Areas are maintained and operated in the most efficient manner consistent with the protection of classified information and in compliance with accreditation requirements. No classified documents, material, recordings, or other information may be removed from the Secure Areas unless so authorized by the CISO. The

~~FBI and~~ CISO shall not reveal to the Government the content of any conversations they may hear among the defense, nor reveal the nature of the documents being reviewed, or the work being generated. The presence of the ~~FBI or the~~ CISO shall not operate to render inapplicable the attorney-client privilege.

21. *Review of Defense Filings.* The Defendant's *pro se* status does not affect or relieve in any way standby counsel's independent obligation to ensure that documents or pleadings containing classified information are filed in accordance with the provisions of this Order. In particular, standby counsel shall review all proposed filings of the Defendant for possible classified information before publicly filing any document. If standby counsel is unable reasonably to determine whether a filing contains or likely contains classified information, standby counsel shall contact the CISO and/or file the document as presumptively classified pending classification review pursuant to the provisions of this Order. Unless and until the CISO or the Government advise standby counsel that the document is unclassified, standby counsel shall treat the document as presumptively classified.

21.22. *Filing of Papers by the Defense.* Any pleading or other document filed by the defense or the Defendant that the Defendant or standby counsel for the Defendant knows or reasonably should know contains classified information as defined in paragraph 2(ab), shall be filed as follows:

a. The document (along with a courtesy electronic copy on CD or DVD) shall be filed by standby counsel under seal with the CISO or an appropriately cleared designee identified by the CISO and shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately

cleared designee shall be considered the date and time of filing and should occur no later than 4:00 p.m. Within a reasonable time after making a submission to the CISO, the defense shall file on the public record in the CM/ECF system a “Notice of Filing” notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing. ~~Standby counsel shall review all proposed filings of the defendant for possible classified information before publicly filing any document. The Defendant’s pro se status does not affect or relieve in any way standby counsel’s independent obligation to ensure that documents or pleadings containing classified information are filed in accordance with the provisions of this Order.~~

b. The CISO shall consult with representatives of the agency or agencies having the relevant classification authority in order to determine whether the pleading or document contains classified information. If the agency or agencies with classification authority determine that the pleading or document contains classified information, the CISO shall ensure the document is marked with the appropriate classification marking and remains under seal. The CISO shall immediately deliver or, if required, arrange for delivery by an appropriately cleared designee under seal to the Court and Government counsel any pleading or document to be filed by the defense that contains classified information, unless the pleading or document is an *ex parte* filing. ~~If standby counsel is unable reasonably to determine whether a filing contains or likely contains classified information, standby counsel shall file the document as presumptively classified pending classification review pursuant to the provisions of this Order.~~

22.23. *Filing of Papers by the Government.* Any pleading or other document filed by the Government that Government counsel knows or reasonably should know contains classified information as defined in paragraph 2(ab), shall be filed as follows:

a. The document (along with a courtesy electronic copy on CD or DVD) shall be filed under seal with the CISO or an appropriately cleared designee and shall be marked, “Filed in Camera and Under Seal with the Classified Information Security Officer.” The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 4:00 p.m. Within a reasonable time after making a submission to the CISO, Government counsel shall file on the public record in the CM/ECF system a “Notice of Filing” notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall ensure the document is marked with the appropriate classification marking and remains under seal. The CISO shall immediately deliver under seal or, if required, arrange for delivery by an appropriately cleared designee to the Court and to the Secure Area used by the defense and the Defendant any pleading or document to be filed by the Government that contains classified information, unless the pleading or document is an *ex parte* filing.

23-24. *Record and Maintenance of Classified Filings.* The CISO shall maintain a separate sealed record for those materials that are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

24-25. *Classification Review.* With respect to classified filings described in paragraphs 2022(b) and 2123(b), except *ex parte* filings or filings under seal, and with respect to classified orders of the Court, the agency having relevant classification authority shall conduct a classification review and prepare a redacted version of the filings and orders for public filing on the docket. The Unless and until the Court orders otherwise, the classification review shall be

completed (i) for filings and orders of 10 pages or fewer, within ~~one~~ week; (ii) for filings and orders of 25 pages or fewer, within two weeks; and (iii) for filings of greater than 25 pages, within three weeks. Attachments containing classified information will not be subject to classification review and will be filed under seal, unless otherwise ordered by the Court. Any attachments subject to classification review will be included in the page counts above, except documents that have previously undergone classification review. These time periods shall begin to run upon the agency receiving the document from the CISO or from Government counsel. The Government shall promptly notify the Court if a particular classification review cannot reasonably be completed within these time periods and may request additional time. The Court may shorten the timeframes set forth above as this case gets closer to trial.

25.26. *The Classified Information Procedures Act.* Procedures for public disclosure of classified information in this case shall be those established by CIPA. The defense and the Defendant shall comply with the requirements of CIPA Section 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the defense and the Defendant shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to Government counsel and until the Government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the Government to appeal any adverse determination under CIPA Section 7 has expired or any appeal under Section 7 by the Government is decided. Pretrial conferences involving classified information shall be conducted *in camera* in the interest of the national security, be attended only by persons granted access to classified

information and a need to know, and the transcripts of such proceedings shall be maintained under seal.

26-27. *Access to Classified Information.* In the interest of the national security, representatives of the defense granted access to classified information and the Defendant shall have access to classified information only as follows:

a. All classified information produced by the Government to counsel for the Defendant in discovery or otherwise, and all classified information possessed, created or maintained by the defense or the Defendant, including notes and any other work product, shall be stored, maintained and used only in the Secure Areas established by the FBI and CISO, unless otherwise authorized by the CISO.

b. *Special procedures for audio recordings.* Any classified audio recordings that the Government discloses to the defense or the Defendant shall be maintained by the FBI and CISO in the Secure Areas. Such recordings may be reviewed only on a stand-alone, non-networked computer or other device within the Secure Areas that does not have the capability to duplicate or transmit information. The defense or the Defendant must use headphones to review such recordings and the headphones must be wired and not have any wireless capability.

c. The defense shall have free access to the classified information made available to them, and the Defendant shall have free access to the classified information made available to him in accordance with the provision of this Order, in the Secure Areas established by the FBI and CISO and shall be allowed to take notes and prepare documents with respect to those materials.

d. No representative of the defense (including but not limited to standby counsel, investigators, paralegals, translators, experts, and witnesses) or the Defendant shall copy or reproduce any classified information in any manner or form, except with the approval of the CISO and in accordance with the procedures established by the CISO for the operation of the Secure Area.

e. All documents prepared by the defense or the Defendant (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in the Secure Areas on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, thumb drives, discs, CDs, DVDs exhibits, and electronic or digital copies) that may contain classified information shall be maintained in the Secure Areas unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to Government counsel or any other party.

f. The defense and the Defendant shall discuss classified information only within the Secure Areas or in an area authorized by the CISO.

g. The defense and the Defendant shall not disclose, without prior approval of the Court, classified information to any person not named in this Order except to the Court, Court personnel, and government personnel identified by the CISO as having the appropriate clearances and the need to know. Government counsel shall be given an opportunity to be heard in response to any defense or Defendant's request for disclosure to a person not identified in this Order. Any person approved by this Court for access to classified information under this paragraph shall be

required to obtain the appropriate security clearance, to sign and submit to this Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, the Department of Justice shall promptly seek to obtain security clearances for them at the request of standby counsel or the Defendant. As set forth above, the defense and the Defendant shall not disclose classified information, even to an individual with the appropriate security clearance, without following the procedure referenced in paragraph ~~17~~18.

h. The defense and the Defendant shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the Internet and email, or in the presence of any person who has not been granted access to classified information by the Court.

i. Any documents written by the defense or the Defendant that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

j. The defense shall not disclose classified information to the Defendant—other than materials marked “Provided to JOSHUA ADAM SCHULTE in *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (JMF)”—absent written permission from the Government.

~~27-28~~28. *Contacting U.S. Intelligence Agency Employees*. The employment and/or affiliation of certain individuals with a U.S. Intelligence Agency and/or their responsibilities at the U.S. Intelligence Agency may constitute classified or highly sensitive facts. As a result, if the defense

or the Defendant would like to contact individuals who may be employed by or affiliated with a U.S. Intelligence Agency (“Intelligence Agency Employees”), the following procedures apply:

a. The CISO is the point of contact for the purpose of facilitating contact between the defense or the Defendant and Intelligence Agency Employees. If the defense or the Defendant would like to contact Intelligence Agency Employees, the name of any such person must be provided to the CISO through properly secured channels.

b. The CISO will subsequently contact via a secure line a designated employee or employees (the “Designated Employee(s)”) at the U.S. Intelligence Agency who will be walled off from the prosecution team. The Designated Employee(s) will notify the Intelligence Agency Employee of the defense or the Defendant’s request to contact and/or interview him or her.

c. If an Intelligence Agency Employee agrees to be contacted and/or interviewed by the defense, the CISO will coordinate with the defense and with the Intelligence Agency Employee regarding logistics (e.g., timing and location) of the proposed interview(s). Classified information may be discussed with the Intelligence Agency Employees only in a SCIF or via secure telephonic or video communications.

28.29. Any unauthorized disclosure or mishandling of classified information may constitute violations of federal criminal law. In addition, any violation of the terms of this Order shall be brought immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual’s access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention, or handling of classified documents or information could cause serious damage, and in some cases exceptionally grave

damage to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. The purpose of this Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it.

~~29.30.~~ All classified documents and information to which the defense or the Defendant have access in this case are now and will remain the property of the United States. Upon request by the CISO, all persons shall return to the CISO all classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information. The notes, summaries, and other documents prepared by the defense or the Defendant that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of the case. At the conclusion of this case, including any appeals or ancillary proceedings thereto, all such notes, summaries, and other documents are to be destroyed by the CISO in the presence of standby counsel for the Defendant if they choose to be present. Even upon the conclusion of this case, the parties, counsel, and any of their representatives or associates to whom classified documents or information was disclosed, remain obligated to protect against the unauthorized disclosure of any classified information learned during the course of the proceedings, as described herein.

Procedures Relating to the Defendant's Access to the Secure Areas

~~30.31.~~ ~~On or about November 3, 2021, the Court entered an order advising that the Court had arranged with the U.S. Marshal for the Southern District of New York for the Defendant to visit the courthouse Sensitive Compartmented Information Facility ("SCIF"), i.e., one of the Secure Areas described in this Order, twice weekly for eight hours per day. The schedule for the~~

Defendant's visits to the Courthouse SCIF are to be coordinated among the U.S. Marshals ServiceUSMS, the FBI, the U.S. Attorney's Office, and standby counsel, and the CISO and the Court are to be notified of the schedule. Standby counsel or a cleared paralegal under the direction and supervision of standby counsel shall accompanybe reasonably available to the Defendant at all times when he is in the Secure Area in order to, among other things, facilitate his access to Classified Information in order to prepare his defense.

~~31.32.~~ Standby counsel will be screened for electronic devices prior to entering the SCIF.

The Secure Area contains equipment (the "Computer Equipment") to allow the ~~defendant~~Defendant and cleared ~~defense~~standby counsel to review the Classified Information produced by the Government. The Computer Equipment shall be used only for purposes of preparing the defense, and is enabled to log computer activity occurring on the equipment and is equipped with security measures. These logs may be reviewed by law enforcement agents or personnel who are not involved in the prosecution of the ~~defendant~~Defendant (the "Wall Team"). In the event the Wall Team determines the Computer Equipment has been used in an unauthorized manner, including by attempting to circumvent any security measures or logging features, the Wall Agent will report that information to the CISO, who will notify the Court for further action.

~~32.33.~~ When the ~~defendant~~Defendant is present in the Secure Area, the Secure Area will be monitored for security purposes through closed circuit television ("CCTV") by the Marshals and an authorized FBI agent for all scheduled productions. The CCTV will allow only for visual monitoring of the ~~defendant~~Defendant and cleared defense counsel, and will not include audio. The CCTV will not be recorded. Should any Marshal or FBI agent hear any conversation between the ~~defendant~~Defendant and any of his counsel, those conversations will not be communicated to

any member of the government prosecution team, including, but not limited to attorneys, agents, and support staff.

~~33.34. The—Unless the Court orders otherwise, the~~ Defendant will be ~~in full restraints~~ subject to appropriate security measures to be determined by USMS during the time he is in the SCIF ~~and secured to a bolt in the floor.~~ The Defendant will be stripped searched after departing the SCIF at the conclusion of each session. ~~Standby counsel will sign a waiver of liability due to the fact she will be alone and in close proximity to the Defendant.~~ The USMS ~~reserves the right to~~ may terminate ~~these meetings~~ any session if security issues arise during ~~any~~ the session.

~~34.35.~~ On September 23, 2021, the Court issued an Order (Dkt. Entry No. 518) directing, among other things, that the parties schedule and hold a telephone call twice a month to meet and confer about discovery and other issues, to take place at a mutually convenient time during the ~~defendant's~~ Defendant's regularly scheduled SCIF hours and with the participation of standby counsel at the discretion of the ~~defendant~~ Defendant and standby counsel. These calls may be held using a teleconference facility and may be recorded by the Government. *See also* Dec. 20, 2021 Tr. at 38-40. The Defendant may not personally place or receive phone calls from the SCIF and shall only use the SCIF phone with the assistance of standby counsel or cleared staff working on this matter at the direction and under the supervision of standby counsel, who will place and receive calls for the Defendant. ~~The Defendant shall use the telephone in the SCIF only to speak with standby counsel or counsel for the Government.~~ Standby counsel or cleared staff working on this matter at the direction and under the supervision of standby counsel shall assist the ~~defendant~~ Defendant in joining teleconference calls directed by the September 23, 2021 Order and this Order. The Government will endeavor to identify the dates of these calls in advance upon

receiving the ~~defendant's~~Defendant's SCIF schedule from the USMS, and may schedule such a call by giving at least 24 hours' notice to standby counsel or by any other means that reasonably gives the Defendant notice. As directed above, the Defendant shall not disclose classified information on telephone calls that are not cleared for classified communications.

Concluding Provisions

~~35.36.~~ Nothing contained in this Order shall be construed as a waiver of any right of the Defendant. No admission made by the Defendant or his standby counsel during pretrial conferences may be used against the Defendant unless it is in writing and signed by the Defendant. *See* CIPA § 2.

~~36.37.~~ A copy of this Order shall be issued forthwith to standby counsel for the Defendant who shall be responsible for advising the Defendant and representatives of the defense of the contents of this Order. Standby counsel for the Defendant, the Defendant, and any other representatives of the defense who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 15 of this Order, and the Defendant and standby counsel for the Defendant shall file executed originals of such documents with the Court and the CISO and serve an executed original upon the government. The execution and filing of the Memorandum of Understanding is a condition precedent for the Defendant, standby counsel for the Defendant, and any other representative of the defense to have access to classified information.

~~Dated:~~ _____
Dated: February 18, 2022

New York, New York

SO ORDERED:

THE HONORABLE JESSE M. FURMAN
UNITED STATES DISTRICT JUDGE

DRAFT

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (JMF)

**MEMORANDUM OF UNDERSTANDING REGARDING RECEIPT OF
CLASSIFIED INFORMATION**

Having familiarized myself with the applicable statutes, regulations, and orders, including but not limited to, Title 18, United States Code, Sections 793, 794, 798, and 1924; the Intelligence Identities Protection Act, Title 50, United States Code, Section 3121 ; Title 1 8, United States Code, Section 641; Title 50, United States Code, Section 783; and Executive Order 13526, I understand that I may be the recipient of information and documents that concern the present and future security of the United States and which belong to the United States, and that such documents and information together with the methods and sources of collecting it are classified by the United States Government. In consideration for the disclosure of classified information and documents:

(1) I agree that I shall never divulge, publish, or reveal either by word, conduct or any other means, such classified documents and information unless specifically authorized in writing to do so by an authorized representative of the United States Government; or as expressly authorized by the Court pursuant to the Classified Information Procedures Act and ~~the~~any Protective Order entered in United States v. Joshua Adam Schulte, S3 17 Cr. 548 (JMF).

(2) I agree that this Memorandum will remain forever binding on me.

(3) I have received, read, and understand the Amended Protective ~~Order~~ Order Regarding Classified Information entered by the United States District Court for the Southern District of New York on _____, 2018~~2022~~, in United States v. Joshua Adam Schulte, S3 17 Cr. 548 (JMF), relating to classified information, and I agree to comply with the provisions thereof.

(4) I understand that any prior contractual obligations that may bind me to continue to protect classified information remain in full force and effect, and are not superseded by this Memorandum of Understanding. Additionally, I understand that this Memorandum of Understanding does not absolve me of any criminal or civil penalties that may otherwise be imposed upon me as a result of my unauthorized disclosure of classified information.

Sabrina Shroff, Esq.
Standby Counsel for the Defendant

Date

Deborah Colson, Esq.
Standby Counsel for the Defendant

Date

Joshua Adam Schulte
Defendant

Date